Direct stakeholders:

Police agency in Georgia:

Van Buren: police sergeant guilty?

Government

Main points:

* Nathan Van Buren, a former police sergeant, ran a license-plate search in a law enforcement computer database in exchange for money.
* **We must decide whether Van Buren also violated the Computer Fraud and Abuse Act of 1986 (CFAA), which makes it illegal “to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter.”**

**Result: He did not. This provision covers those who obtain information from particular areas in the computer—such as files, folders, or databases—to which their computer access does not extend. It does not cover those who, like Van Buren, have improper motives for obtaining information that is otherwise available to them.**

* **This case stems from Van Buren’s time as a police sergeant in Georgia. In the course of his duties, Van Buren crossed paths with a man named Andrew Albo. The deputy chief of Van Buren’s department considered Albo to be “very volatile” and warned officers in the department to deal with him carefully. Notwithstanding that warning, Van Buren developed a friendly relationship with Albo. Or so Van Buren thought when he went to Albo to ask for a personal loan. Unbeknownst to Van Buren, Albo secretly recorded that request and took it to the local sheriff ’s office, where he complained that Van Buren had sought to “shake him down” for cash. The taped conversation made its way to the Federal Bureau of Investigation (FBI), which devised an operation to see how far Van Buren would go for money. The steps were straightforward: Albo would ask Van Buren to search the state law enforcement computer database for a license plate purportedly belonging to a woman whom Albo had met at a local strip club. Albo, no stranger to legal troubles, would tell Van Buren that he wanted to ensure that the woman was not in fact an undercover officer. In return for the search, Albo would pay Van Buren around $5,000.** **Things went according to plan. Van Buren used his patrol-car computer to access the law enforcement database with his valid credentials. He searched the database for the license plate that Albo had provided. After obtaining the FBI-created license-plate entry, Van Buren told Albo that he had information to share.**
* Van Buren appealed to the Eleventh Circuit, arguing that the “exceeds authorized access” clause applies only to those who obtain information to which their computer access does not extend, not to those who misuse access that they otherwise have. While several Circuits see the clause Van Buren’s way, the Eleventh Circuit is among those that have taken a broader view.2 Consistent with its Circuit precedent, the panel held that Van Buren had violated the CFAA by accessing the law enforcement database for an “inappropriate reason.”
* He was also charged and convicted of honest-services wire fraud and a felony
* Both Van Buren and the Government raise a host of policy arguments to support their respective interpretations. But we start where we always do: with the text of the statute. Here, the most relevant text is the phrase “exceeds authorized access,” which means “to access a computer with authorization and to use such access to obtain . . . information in the computer that the accesser is not entitled so to obtain.” §1030(e)(6). The parties agree that Van Buren “access[ed] a computer with authorization” when he used his patrol-car computer and valid credentials to log into the law enforcement database. They also agree that Van Buren “obtain[ed] . . . information in the computer” when he acquired the license-plate record for Albo. The dispute is whether Van Buren was “entitled so to obtain” the record. “Entitle” means “to give . . . a title, right, or claim to something.” Random House Dictionary of the English Language 649 (2d ed. 1987). See also Black’s Law Dictionary 477 (5th ed. 1979) (“to give a right or legal title to”). The parties agree that Van Buren had been given the right to acquire license-plate information—that is, he was “entitled to obtain” it—from the law enforcement computer database. But was Van Buren “entitled so to obtain” the license-plate information, as the statute requires?
* Word “so”: Van Buren’s account of “so”—namely, that “so” references the previously stated “manner or circumstance” in the text of §1030(e)(6) itself—is more plausible than the Government’s. “So” is not a free-floating term that provides a hook for any limitation stated anywhere. It refers to a stated, identifiable proposition from the “preceding” text; indeed, “so” typically “[r]epresent[s]” a “word or phrase already employed,” thereby avoiding the need for repetition. 15 Oxford English Dictionary, at 887; see Webster’s Third New International Dictionary 2160 (1986) (so “often used as a substitute . . . to express the idea of a preceding phrase”). Myriad federal statutes illustrate this ordinary usage.3 We agree with Van Buren: The phrase “is not entitled so to obtain” is best read to refer to information that a person is not entitled to obtain by using a computer that he is authorized to access.4
* After this government argued the word so would not disrupt meaning, even then the rule against superfluity means that its interpretation wins.
* computer system,” such as files, folders, or databases.6 It is thus consistent with that meaning to equate “exceed[ing] authorized access” with the act of entering a part of the system to which a computer user lacks access privileges.7

end of case:

* Both the common law and statutory law have long punished those who exceed the scope of consent when using property that belongs to others. A valet, for example, may take possession of a person’s car to park it, but he cannot take it for a joyride. The Computer Fraud and Abuse Act extends that principle to computers and information. The Act prohibits exceeding the scope of consent when using a computer that belongs to another person. Specifically, it punishes anyone who “intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains” information from that computer. 18 U. S. C. §1030(a)(2). As a police officer, Nathan Van Buren had permission to retrieve license-plate information from a government database, but only for law enforcement purposes. Van Buren disregarded this limitation when, in exchange for several thousand dollars, he used the database in an attempt to unmask a potential undercover officer. The question here is straightforward: Would an ordinary reader of the English language understand Van Buren to have “exceed[ed] authorized access” to the database when he used it under circumstances that were expressly forbidden? In my view, the answer is yes. The necessary precondition that permitted him to obtain that data was absent. The Court does not dispute that the phrase “exceeds authorized access” readily encompasses Van Buren’s conduct. It notes, instead, that the statute includes a definition for that phrase and that “we must follow that definition, even if it varies from a term’s ordinary meaning.” Tanzin v. Tanvir, 592 U. S. \_\_\_, \_\_\_ (2020) (slip op., at 3) (internal quotation marks omitted). The problem for the majority view, however, is that the text, ordinary principles of property law, and statutory history establish that the definitional provision is quite consistent with the term it defines

Case synopsis

The main stakeholders in this case are the government agencies as a whole, the Georgia police department, and the opposite side or the defendant including Involves Van Buren and his lawyer. The main case revolves around the misuse of computer access to search for something that was not lawful or should be done even if it was ultimately done with good intentions(debatable). The case stems from from when van Buren was a police sergeant in Georgia; “**course of his duties, Van Buren crossed paths with a man named Andrew Albo. The deputy chief of Van Buren’s department considered Albo to be “very volatile” and warned officers in the department to deal with him carefully. Notwithstanding that warning, Van Buren developed a friendly relationship with Albo. Or so Van Buren thought when he went to Albo to ask for a personal loan. Unbeknownst to Van Buren, Albo secretly recorded that request and took it to the local sheriff ’s office, where he complained that Van Buren had sought to “shake him down” for cash. The taped conversation made its way to the Federal Bureau of Investigation (FBI), which devised an operation to see how far Van Buren would go for money. The steps were straightforward: Albo would ask Van Buren to search the state law enforcement computer database for a license plate purportedly belonging to a woman whom Albo had met at a local strip club. Albo, no stranger to legal troubles, would tell Van Buren that he wanted to ensure that the woman was not in fact an undercover officer. In return for the search, Albo would pay Van Buren around $5,000.** **Things went according to plan. Van Buren used his patrol-car computer to access the law enforcement database with his valid credentials. He searched the database for the license plate that Albo had provided. After obtaining the FBI-created license-plate entry, Van Buren told Albo that he had information to share”.**

To summarize the case had three rulings that change the way the interpretation from the initial rule of, **“to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter.”.** The first ruling was the word “so” which ultimately helps the third and last ruling, in short so was determined to be connected to the word entitled in that it without the word so there would be limitations to what is entitled.

The second ruling was related to the nature of searching for something not entitled to obtain, it turned out that he is able to search whatever he wants since he does have the official credentials to do so, in contrast the rule would apply for someone external without the credentials to do so.

The last ruling was over the word “entitled”, it decided whether or not Buren was entitled to the information and after careful examination they determined entitled was the “proper grounds” and Van Buren was in the proper grounds to search and investigate since he did so in a controlled space inside his office. All these rulings together declared him not guilty. He was also charged and convicted of honest-services wire fraud and a felony at the end of all the cases

Personal ethics:

I think the use of Van Buren use of information was ultimately unlawful since the use of his credentials to pursue information that was not clearly related to a case and was used for personal gain was definitely not within the scope of a law. Although I can see the other side of the story and understand that the police agency also tricked to some degree Van Buren into doing the unlawful search it is still an ultimately breaking the law and prevented a police officer from doing an unlawful search in some other means instead of a controlled situation. However in this case the main objective analyzing if the rules were followed during the search based on the law; “**We must decide whether Van Buren also violated the Computer Fraud and Abuse Act of 1986 (CFAA), which makes it illegal “to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter.”** After reading the case I understand their results and have also arrived to the conclusion of not guilty since the wording use is inaccurate even though ultimately there was an unlawful search, he did follow the rules above and did not search for anything he was not supposed to do.

Professional ethics:

The ACM Code of Ethics emphasizes integrity, honesty, and the responsible use of technology, all of which are relevant to Van Buren’s case. He misused his authorized access for personal gain, violating ethical standards expected of law enforcement officers handling sensitive data. The ACM Code highlights that computing professionals should use their access responsibly and avoid actions that could undermine public trust. While Van Buren had legitimate credentials to access the database, his intent was not for law enforcement purposes but for personal financial benefit, which breaches professional ethics. The ACM Code stresses the importance of avoiding harm and maintaining professional integrity, both of which were compromised in this situation.

One key ethical concern in this case is the misuse of privileged access. The ACM Code states that professionals should not abuse their authority or access to systems for personal gain. Van Buren’s actions, even if legally permissible based on the interpretation of “entitled,” were ethically problematic because they involved a breach of trust and professional responsibility. The act of searching for information in exchange for money, even within a controlled environment, raises concerns about corruption and the responsible use of law enforcement databases. If such actions were normalized, it could lead to a loss of public trust in the ability of law enforcement to use sensitive data ethically. Furthermore, ethical computing professionals should recognize the broader implications of their actions, as even seemingly minor breaches of ethics can contribute to systemic issues in organizations and society.

Additionally, the ACM Code promotes transparency, accountability, and adherence to policies and laws governing computer access, all of which were lacking in Van Buren’s actions. He failed to uphold the trust placed in him as a law enforcement officer by engaging in a transaction that prioritized personal gain over ethical duty. Instead of misusing his access, the correct course of action would have been to refuse the request, report the bribery attempt, and uphold professional integrity. Even though the court ultimately ruled him not guilty under the Computer Fraud and Abuse Act due to a technicality in wording, his actions still violated the principles of responsible computing, accountability, and ethical conduct.